1/4/1
DIALOG(R)File 351:Derwent WPI


IM- *Image available*
AA- 1998-261842/199823|
XR- <XRPX> N98-206389|
TI- **Firewall for controlling access between two computer systems - uses tunnelling mechanism to operate on both sides of wall to set up outside-in connections when requested by trusted objects or users outside wall**|
PA- INT BUSINESS MACHINES CORP (IBMC ); IBM UK LTD (IBMC )|
AU- <INVENTORS> JADE P; MOORE V S; RAO A M; WALTERS G R|
NC- 029|
NP- 011|
PN- WO 9818248 A1 19980430 WO 97GB2712 A 19971002 199823 B|
PN- EP 932965 A1 19990804 EP 97943996 A 19971002 199935
<AN> WO 97GB2712 A 19971002
PN- BR 9705094 A 19990629 BR 975094 A 19971020 199937
PN- CZ 9901387 A3 19990811 WO 97GB2712 A 19971002 199937
<AN> CZ 991387 A 19971002
PN- US 5944823 A 19990831 US 96731800 A 19961021 199942
PN- BR 9712635 A 19991026 BR 9712635 A 19971002 200009
<AN> WO 97GB2712 A 19971002
PN- TW 362177 A 19990621 TW 97107568 A 19970603 200028
PN- US 6061797 A 20000509 US 96731800 A 19961021 200030
<AN> US 98132915 A 19980812
PN- **JP 2000505270 W 20000425** WO 97GB2712 A 19971002 200031
<AN> JP 98519056 A 19971002
PN- HU 200000336 A2 20000628 WO 97GB2712 A 19971002 200039
<AN> HU 2000336 A 19971002
PN- KR 2000048930 A 20000725 WO 97GB2712 A 19971002 200116
<AN> KR 99702966 A 19990406|
AN- <LOCAL> WO 97GB2712 A 19971002; EP 97943996 A 19971002; WO 97GB2712 A 19971002; BR 975094 A 19971020; WO 97GB2712 A 19971002; CZ 991387 A 19971002; US 96731800 A 19961021; BR 9712635 A 19971002; WO 97GB2712 A 19971002; TW 97107568 A 19970603; US 96731800 A 19961021; US 98132915 A 19980812; WO 97GB2712 A 19971002; JP 98519056 A 19971002; WO 97GB2712 A 19971002; HU 2000336 A 19971002; WO 97GB2712 A 19971002; KR 99702966 A 19990406|
AN- <PR> US 96731800 A 19961021; US 98132915 A 19980812|
CT- No-SR.Pub|
FD- WO 9818248 A1 H04L-029/06
<DS> (National): BR CA CN CZ HU JP KR PL RU
<DS> (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE
FD- EP 932965 A1 H04L-029/06 Based on patent WO 9818248
<DS> (Regional): AT BE CH DE ES FR GB IE IT LI NL SE

FD- CZ 9901387 A3 H04L-029/06 Based on patent WO 9818248
FD- BR 9712635 A H04L-029/06 Based on patent WO 9818248
FD- US 6061797 A G06F-012/14 Cont of application US 96731800
Cont of patent US 5944823
FD- JP 2000505270 W H04L-012/66 Based on patent WO 9818248
FD- HU 200000336 A2 H04L-029/06 Based on patent WO 9818248
FD- KR 2000048930 A H04L-029/06 Based on patent WO 9818248|
LA- WO 9818248(E<PG> 18); EP 932965(E); JP 2000505270(26)|
DS- <NATIONAL> BR CA CN CZ HU JP KR PL RU|
DS- <REGIONAL> AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LU; MC; NL; PT; SE; LI|
AB- <BASIC> WO 9818248 A

The tunnelling apparatus for a data communication network including a fire-wall (1) which defines outside and inside regions and forms a security barrier. This prevents objects in the outside region from accessing objects in the inside region, while objects in the inside region are permitted to access objects in the outside region. An outside interface computer (3) is located in the outside region, and an inside interface computer (2) interfaces between the firewall and objects in the inside region.

A device in both the computers is provided for determining the identities of predetermined trusted objects in the inside region to which access is allowed from the outside region. A device in the outside computer responds to a request sent from an object in the outside region and cooperates with the determining device to check if the request is directed to one of the trusted objects. If the request is so directed the request is routed to the inside interface computer. A device in both interface computers responds to the request directed to the trusted object for forming a data communication connection to the outside object. The segments of the data connection located in the inside region and extending through the firewall are formed under the exclusive control of the inside interface computer. A segment of the data communication connection extends from the outside interface computer to the object that sent the request and is formed under the control of the outside interface computer.

USE - For isolating computer an network resources inside firewall from networks, computers and computer applications outside wall. ADVANTAGE - Provides for special 'tunnelling' access from inside services to outside services.

Dwg.1/5|

DE- <TITLE TERMS> FIREWALL; CONTROL; ACCESS; TWO; COMPUTER; SYSTEM; TUNNEL; MECHANISM; OPERATE; SIDE; WALL; SET; UP; CONNECT; REQUEST; OBJECT; USER ; WALL|
DC- T01; W01|
IC- <MAIN> G06F-011/00; G06F-012/14; G06F-013/10; H04L-012/66; H04L-029/06|
IC- <ADDITIONAL> G06F-013/00; G06F-013/16; H04L-009/32; H04L-012/28; H04L-012/46; H04L-012/56|

MC- <EPI> T01-J12C; T01-L09; W01-A07G|
FS- EPI||

(19)日本国特許庁(JP)

(12)公表特許公報（A）

(11)特許出願公表番号

特表２０００－５０５２７０
(Ｐ２０００－５０５２７０Ａ)
(43)公表日　平成12年4月25日(2000.4.25)

| (51)Int.Cl.⁷ | | 識別記号 | FI | | | テーマコード(参考) |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 12/66 | | Ｈ０４Ｌ | 11/20 | Ｂ | |
| Ｇ０６Ｆ | 13/00 | ３５１ | Ｇ０６Ｆ | 13/00 | ３５１　Ｚ | |
| Ｈ０４Ｌ | 12/28 | | Ｈ０４Ｌ | 11/20 | １０２　Ｚ | |
| | 12/46 | | | 11/00 | ３１０　Ｃ | |
| | 12/56 | | | | | |

審査請求　有　予備審査請求　有　(全２６頁)

(21)出願番号　特願平10-519056
(86)(22)出願日　平成9年10月2日(1997.10.2)
(85)翻訳文提出日　平成11年4月14日(1999.4.14)
(86)国際出願番号　PCT/GB97/02712
(87)国際公開番号　WO98/18248
(87)国際公開日　平成10年4月30日(1998.4.30)
(31)優先権主張番号　08/731,800
(32)優先日　平成8年10月21日(1996.10.21)
(33)優先権主張国　米国(US)
(81)指定国　EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), BR, CA, CN, CZ, HU, JP, KR, PL, RU

(71)出願人　インターナショナル・ビジネス・マシーンズ・コーポレーション
アメリカ合衆国10504、ニューヨーク州アーモンク（番地なし）
(72)発明者　ジェイド、プラシャント
アメリカ合衆国ペンシルバニア州リドリー・パーク、イースト・ヘンクル・アヴェニュー　515
(72)発明者　ムーア、ビクター、スチュアート
アメリカ合衆国フロリダ州ボイントン・ビーチ、パイン・トリー・ドライブ　4739
(74)代理人　弁理士　坂口　博　(外1名)

最終頁に続く

(54)【発明の名称】ファイアウォールを通過するコンピュータ資源への外部アクセス

(57)【要約】
ファイアウォールが、ファイアウォール内部のコンピュータ資源およびネットワーク資源を、ファイアウォール外部のコンピュータおよびコンピュータ・アプリケーションから分離する。典型的には、内部資源は私有データベースおよびローカル・エリア・ネットワーク（ＬＡＮ）が考えられ、外部オブジェクトはインターネットなどの公衆通信ネットワークを介して操作する個人およびコンピュータ・アプリケーションを含む。通例、ファイアウォールは内部のユーザまたはオブジェクトが外部のオブジェクトまたはネットワークへの接続を開始することはできるようにするが、その逆方向、すなわち外部から内部への接続は行われないようにする。開示の本発明は、ファイアウォールの両側で動作し、ファイアウォール外部の特定の「トラステッド」個人、オブジェクト、またはアプリケーションによって要求された場合に、そのような「外部から内部への」接続を確立する特別な「トンネル」機構を提供する。本発明の意図は、「トンネル」接続（外部から有効に要求されたファイアウォールを介した接続）を確立するのに必要な資源を最小限に

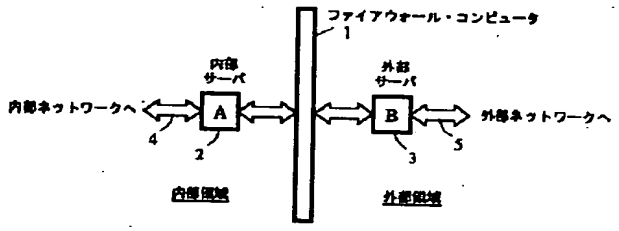



FIG. 1

【特許請求の範囲】

１．ファイアウォールが内部領域と外部領域を規定し、前記外部領域内のオブジェクトが前記内部領域内のオブジェクトへのアクセスを直接開始するのを防止するセキュリティ障壁を形成すると同時に、前記内部領域内のオブジェクトが前記外部領域内のオブジェクトへのアクセスを直接開始し、アクセスを獲得することを許すファイアウォール（１）を含むデータ通信ネットワークのためのトンネル装置であって、

前記ファイアウォール（１）と前記外部領域内のオブジェクトとの間のインタフェースをとる、前記外部領域内の外部インタフェース・コンピュータ（３）と、

前記ファイアウォール（１）と前記内部領域内のオブジェクトとの間のインタフェースをとる、前記内部領域内の内部インタフェース・コンピュータ（２）と、

前記内部と外部の両方のインタフェース・コンピュータにおいて、前記外部領域からのアクセスが許可されている前記内部領域内の所定のトラステッド・オブジェクトの識別情報を確認する手段と、

前記外部インタフェース・コンピュータにおいて、前記外部領域内のオブジェクトから送られた要求に応答して、前記確認手段と協調して、前記要求が前記トラステッド・オブジェクトのうちの１つのオブジェクトに宛てられたものであるか否かを判断し、前記要求がそのように宛てられたものであ

る場合、前記要求を前記内部インタフェース・コンピュータにルーティングする手段と、

前記内部と外部の両方のインタフェース・コンピュータにおいて、前記トラステッド・オブジェクトのうちの前記１つのオブジェクトに宛てられた前記要求に応答して、前記トラステッド・オブジェクトのうちの前記１つのオブジェクトとそれぞれの前記要求を送った外部オブジェクトとの間のデータ通信接続を形成する手段とを含み、前記データ通信接続のうちの前記内部領域にあるセグメントと前記ファイアウォールを通って延びるセグメントが前記内部インタフェース・コ

ンピュータの排他的制御下で形成され、前記データ通信接続のうちの前記外部インタフェース・コンピュータから前記要求を送った前記オブジェクトまでのセグメントが前記外部インタフェース・コンピュータの制御下で形成されるトンネル装置。

２．前記トラステッド・オブジェクトの識別情報を確認する前記手段が、前記内部インタフェース・コンピュータにおいて、前記トラステッド・オブジェクトをリストするテーブルの作成と維持を行う手段と、前記テーブル・リストのコピーを前記ファイアウォール（１）を介して前記外部インタフェース・コンピュータ（３）に転送する手段と、前記外部インタフェース・コンピュータにおいて、前記コピーされたテーブル・リストの記憶と参照を行う手段とを含む、請求項１に記載のトンネル装置。

３．前記内部インタフェース・コンピュータが、前記外部インタフェース・コンピュータまでの専用制御接続の確立と維持を行う手段を含み、前記専用制御接続が前記要求を前記外部インタフェース・コンピュータから前記内部インタフェース・コンピュータに伝送するために使用される、請求項１または２に記載のトンネル装置。

４．トラステッド・オブジェクトの前記テーブル内の各項目（３０）が、前記内部領域内のオブジェクトを識別する第１の情報と、それぞれの前記オブジェクトに割り当てられたデータ通信ポートを識別する第２の情報と、前記ポートを介してデータを伝送するために使用されるデータ通信プロトコルを識別する第３の情報とから成る、請求項２に記載のトンネル装置。

５．前記トラステッド・オブジェクトの識別情報を確認する前記手段と、データ通信接続を形成する前記手段とが、

前記内部と外部の両方のインタフェース・コンピュータ内で実行され、前記確認手段と前記形成手段を構成要素として含む、トンネル・アプリケーション・プログラムと、

前記要求を前記内部インタフェース・コンピュータにルーティングする前記手段が、前記トンネル・アプリケーション・プログラムの第３の構成要素を含む、

請求項１に記載のトンネル装置。

６．前記内部領域と外部領域がそれぞれ内部および外部のデータ通信ネットワークを含み、前記内部および外部のインタ

フェース・コンピュータが前記ファイアウォールと前記内部ネットワークおよび外部ネットワークのノードとの間にそれぞれ接続された、請求項１に記載のトンネル装置。

７．ファイアウォール外部のデータ処理オブジェクトが前記ファイアウォール内部のデータ処理オブジェクトとのデータ通信接続を確立することができるようにする、コンピュータ可読記憶媒体上に記憶されたトンネル・ソフトウェアであって、

それぞれ前記ファイアウォールの内部と外部に配置され、前記ファイアウォールとそれぞれ前記ファイウォールの内部と外部にある前記オブジェクトとの間のインタフェースをとるコンピュータ上で実行されるように意図された内部および外部のプログラム・セグメントを含み、

前記内部セグメントが、前記内部コンピュータを操作してトラステッド内部オブジェクトのテーブルの作成と維持を行う手段と、前記ファイアウォールと共に前記内部コンピュータを操作して前記外部セグメントに前記テーブルのコピーを供給する手段とを含むソフトウェア。

８．コンピュータ・システム・セキュリティ・ファイアウォール（１）外部のオブジェクトが前記ファイアウォール内部の選択されたオブジェクトへのデータ接続を獲得することができるようにする方法であって、

テーブル内の各項目（３０）が選択されたオブジェクトと前記オブジェクトに割り当てられたデータ通信ポートとそれ

ぞれの前記ポートに割り当てられたデータ通信プロトコルとを識別する情報を含む、前記ファイアウォール（１）内部の選択されたオブジェクトのテーブルの作成と維持を行うステップと、

前記ファイアウォール外部に前記テーブルのコピーを設けるステップと、

外部オブジェクトに前記テーブル内の項目を構成する情報への特定のセキュリティ・クリアランス・アクセスを与えるステップと、

それぞれの前記外部オブジェクトに、前記外部オブジェクトに提供された情報によって規定された前記オブジェクト、ポート、およびプロトコル・エンティティへのアクセスを求める要求を発行させるステップと、

前記ファイアウォールの外部と内部のコンピュータ・システムに、各要求で識別された特定の内部オブジェクトと前記要求を発行した外部オブジェクトとの間にデータ伝送接続を確立させるステップとを含み、前記データ伝送接続のうちの前記ファイアウォールの内部にあるセグメントと前記ファイアウォールを通って延びるセグメントが前記ファイアウォールの内部の前記コンピュータ・システムの排他的制御下で形成される方法。

９．前記内部コンピュータと前記外部コンピュータとの間に専用制御接続を確立するステップと、

前記制御接続を排他的に使用して、前記テーブル内の項目

に対応する情報を含む要求を前記外部コンピュータから前記内部コンピュータに排他的に伝送し、前記ファイアウォールを介した前記データ接続を確立する必要に応じて前記コンピュータ間の通信を持続させるステップとを含む、請求項８に記載の方法。

【発明の詳細な説明】

# ファイアウォールを通過するコンピュータ資源への外部アクセス

## 発明の分野

本発明は、ファイアウォールの外部のオブジェクトからの要求に応答したセキュリティ・ファイアウォール内部のコンピュータ・システムまたはネットワークの資源へのアクセスの提供に関する。

## 発明の背景

ファイアウォールとは、コンピュータ・システムまたはネットワークの資源をそのシステムまたはネットワークの外部のオブジェクトから分離するセキュリティ・システム（ハードウェアまたはソフトウェアあるいはその両方）である。分離された資源は、ファイアウォール内部にあるものとして特徴づけられ、外部装置はファイアウォールの外部にあるとみなされる。一般には、ファイアウォールは、コンピュータおよびそれに付随する周辺装置から成る私設ローカル・エリア・ネットワーク（ＬＡＮ）の周囲にめぐらされたセキュリティ囲いの役割を果たす。

一般に、ファイアウォールは、内部オブジェクトが外部オブジェクトへの接続の要求と受取りを行えるようにする（たとえば内部アプリケーションが外部のインターネット・ノードにアクセスするなど）が、外部オブジェクトが同様の接続を開始するのを防ぐ。

ファイアウォールのセキュリティの目的を完全に無効化しないという制約を条件として、ファイアウォールの外部のオブジェクトが内部資源にアクセスできるようにしたい場合がある。たとえば、ファイアウォール内部の資源を所有する会社の従業員が、公衆ネットワーク（電話網や、その電話網およびインターネットのアクセスポイントなど）を介して、従業員の職場から遠隔にある家庭から（または出張中または休暇中に遠隔地から）「テレコミュート」することができるようにすることが望ましい場合がある。そのために、「承認された（トラステッド）」個人がファイアウォールの外部からファイアウォールの内部の資源（たとえ

ばその従業員の個人データベース）へのアクセスを開始することができるようにすることが望ましい。

発明人等が知る限りでは、外部からの開始または要求に応答したこのようなアクセスは、これまでは、ファイアウォールの内部と外部の両方に重複サーバおよびデータベース記憶域を設けるか、またはファイアウォール自体のメンテナンスの費用をかなり増大させるその他の機構を使用して提供されてきた。たとえば、ファイアウォール内部に記憶されている膨大で頻繁に更新されるデータベースに関するそのような外部重複構成の費用やその他の処理を考えてみればわかる。本発明は、ファイアウォール内部のオブジェクトまたは資源の不要な外部重複なしに、所望の外部アクセスを可能にしようとするものである。

発明の概要

様々な態様により、本発明は、独立請求項に記載され、従属請求項に記載された有利な好ましい特徴を有するトンネル装置、方法、およびコンピュータ・プログラム製品を提供する。

本発明によると、ファイアウォール外部のオブジェクトによって開始された特定のタイプの要求に応答して外部オブジェクトとファイアウォール内部の資源との間に接続を形成するトンネル効果を協調的に生じさせる手段を、ファイアウォールの内部と外部に設ける。このようにして形成された接続は、ファイアウォール内部のオブジェクトからファイアウォール外部の宛先に向けて開始された要求であるかのように、実質的に「ひっくり返して」形成されるという独自の特性を有する。

このような「トンネル」手段が対応する「要求のタイプ」は、現在「トラステッド・ソケット」と呼ばれているものに宛てられた要求である。トラステッド・ソケットとは、ファイアウォールの内部で排他的に作成され、維持されるトラステッド・ソケット・テーブル内の項目である。このテーブルの各項目には、「トラステッド」ポートのアドレス、そのアドレスに事前に関連づけられているプロトコル（たとえばＴＣＰ／ＩＰ、ＮＮＴ

Ｐなどの通信プロトコル）、およびファイアウォール内部のホスト・オブジェクト（たとえばホスト・コンピュータまたはホスト・アプリケーション）の識別情報などが含まれる。したがって、ファイアウォール外部の個人またはオブジェクトがそのような要求を開始するためには、その個人に対して、現在有効なトラステッド・ソケット項目を表す情報を、信用して与えなければならないことを理解されたい。

トラステッド・ソケットのテーブルは、「トンネル・アプリケーション」とファイアウォール内部の他のすべての「アクセス可能」オブジェクト／資源（インタフェース・サーバ内部で実行されている他のアプリケーションを含む）との間のインタフェースをとる内部インタフェース・サーバ上で実行される、「トンネル・アプリケーション」によって（そのサーバへの直接アクセス権を有する適正に許可された個人の制御下で）作成され、維持される。内部インタフェース・サーバは、ファイアウォールと、ファイアウォール外部のすべてのオブジェクトとの間のインタフェースをとる外部インタフェース・サーバとの「制御接続」も確立する。この制御接続には、内部インタフェース・サーバ上で実行されているトンネル・アプリケーションと、外部インタフェース・サーバ上で実行されている対応するトンネル・アプリケーションのみがアクセスすることができる。すなわち、制御接続には、

これらのインタフェース・サーバ上で実行されている他のどのアプリケーションも直接アクセスすることができず、これらのサーバ上に置かれていない内部と外部の両方のオブジェクトはまったくアクセスすることができない。

たとえばトラステッド・ソケット・テーブルが作成または変更されたときや特別な時刻などに、内部インタフェース・サーバから外部インタフェース・サーバにトラステッド・ソケット・テーブルのコピーが転送される。

現在ファイアウォールを介して接続されていない外部オブジェクトが外部インタフェース・サーバに届く要求を出した場合、そのサーバ上のトンネル・アプリケーションは、その要求が現在有効なトラステッド・ソケット項目に宛てられたものかどうかを判断する。有効なトラステッド・ソケット項目に宛てられたもの

でない場合、その要求は無視される。トラステッド・ソケット項目に宛てられたものである場合、その要求は制御接続を介して内部インタフェース・サーバ上のトンネル・アプリケーションに渡される。それと同時に、その要求に関連づけられたプロセス（またはタスク）が外部インタフェース・サーバで生成され、そのプロセス／タスクと要求側オブジェクトとの間に外部接続が確立される。

内部トンネル・アプリケーションは、要求を受け取ると、要求が現在有効なトラステッド・ソケットに対するものかどうかを検証し、そうでなかった場合にはその要求を認めないようにする必要がある場合もある。要求が現在有効なトラステッド・ソケットに対するものである場合、内部トンネル・アプリケーションは、その要求に付随する内部プロセスを生成（または「作成（spawn）」）する。次に、内部トンネル・アプリケーションは、（ａ）「要求された」トラステッド・ソケット項目のポートおよびホスト識別情報に関連づけられた内部資源と、内部インタフェース・サーバとの間の接続を生成し、（ｂ）制御接続を介して外部トンネル・アプリケーション、およびファイアウォール自体を制御するコンピュータと通信し、内部と外部の両方のインタフェース・サーバ上で生成／作成されたタスク間にファイアウォールを通した接続を生成する。内部および外部トンネル・アプリケーションによって生成／作成された接続は制御接続から分離され、要求を出した外部オブジェクトと要求の宛先である内部オブジェクトとの間で双方向に（通常はトラステッド・ソケット・プロトコルによって定義されたパケット形式の）データを伝達するのに有用である。

本発明の上記およびその他の特徴、長所、目的、および利点は、以下の詳細な説明と特許請求の範囲を検討すればよりよく理解できよう。

図面の簡単な説明

第１図は、本発明を適用することができる典型的なファイアウォール環境を示す略図である。

第２図は、上述のトラステッド・ソケット・テーブルの作成と処理を示す流れ図である。

第３図は、本発明のファイアウォール・トンネル・プロセスを示す流れ図である。

第４図は、上述のトラステッド・ソケット・テーブルの好ましい態様を示す図である。

第５図は、本発明によるファイアウォールの内部および外部のトンネル・アプリケーション動作を詳述する流れ図である。

好ましい実施形態の詳細な説明

第１図に、本発明が適用される典型的なファイアウォール環境を示す。ファイアウォール・コンピュータ１が、現在一般的に行われている手続きに従ってファイアウォール・セキュリティ機能を維持する。このコンピュータの、ファイアウォール内部のオブジェクトからファイアウォール外部のオブジェクトに接続を拡張する機能以外の機能は、本発明には影響を及ぼさない（また本質的に本発明に関係がない）。インタフェース・サーバ２および３（それぞれサーバＡおよびＢと符号が付されている）がそれぞれ、１によって形成されたファイアウォールの内部および外部で動作する。サーバＡは、ファイアウォールと、サーバＡ自体内のオブジェクトを含むファイアウォール内部のオブジェクト（ソフトウェア・アプリケーション、ハードウェア体など）とのインタフェースをとる。サーバＢは、ファイアウォールと、サーバＢ自体内の

オブジェクトを含むファイアウォール外部のオブジェクトとの間のインタフェースをとる。

典型的なファイアウォール使用環境では、サーバＡは４に示す接続を介してファイアウォール内部のネットワーク（たとえば私設ローカル・エリア・ネットワーク）に接続し、サーバＢは、５に示す接続を介してファイアウォール外部のネットワーク（たとえばインターネット）に接続する。

この環境構成に本発明を適用する際、サーバＡおよびＢは「トンネル」ソフトウェア・アプリケーションを備え、「トラステッド・ソケット」テーブルのコピーを記憶する。これらの実体（トンネル・アプリケーションとトラステッド・ソケット・テーブル）は本発明固有のものと見なされ、本明細書で説明する。

第２図および第３図に、本発明を推進してサーバＡおよびＢで実行される（トンネル）プロセスを示す。

第２図の１０に示すように、トラステッド・ソケット・テーブル（第４図を参照しながら後述する）が作成され、サーバＡ（またはサーバＡが容易にアクセスできる記憶域）に記憶される。１１に示すように、サーバＡは、ファイアウォール（コンピュータ）を介したサーバＢとの特別な「制御接続」を形成し、この制御接続を介してトラステッド・ソケット・テーブルのコピーをサーバＢに渡す。この制御接続も本発明の一部と見なされ、前述のトンネル・アプリケーションどうしが有効に相互通信するために使用され、それによって、外

部オブジェクトから受け取った要求に応答して、ファイアウォールの内部と外部のオブジェクトの間のその他の接続（以下「データ接続」と呼ぶ）が形成される。

ファイアウォールを通過して延びるこれらのデータ接続の各セグメントは、それらのセグメントの形成に使用される制御接続から完全に分離され、常に、ファイアウォール内部で実行されているプロセスの制御下で形成される。外部要求によって内部オブジェクトへのデータ接続の形成が行われるためには、その要求がトラステッド・ソケット・テーブル内の項目に宛てられなければならず、その有効性が検証されなければならない。無効であると判明した外部要求は無視され、それによって、ファイアウォールおよびその内部資源は、無効な要求情報を有する外部要求者にとって実質的に不可視になり、アクセス不能になる。逆に、有効な要求は、トラステッド・ソケット・テーブル内の現在有効な項目の特権的知識を有する個人（たとえば内部資源の所有者の在宅従業員など）の指示でのみ発行可能であることを理解されたい。

第３図で、サーバＢがサーバＡから送られたトラステッド・ソケツト・テーブルのコピーを受け取って記憶した後、サーバＡおよびＢで実行されるトンネル機能について説明する。

２０に示すように、サーバＢ（内のトンネル・アプリケーション）が、トンネル操作、すなわち要求で指定されている内部「ホスト」オブジェクトと要求の送

り元である外部オブジェクトとの間のデータ接続の作成を、有効に求める外部要求の受信を待つ。要求を受け取ると（第３図の２１）、Ｂ（にあるトンネル・アプリケーション）は、その要求を調べて有効な要求であることを検証する（第３図の決定ブロック２２）。この最後に述べた機能に関しては、サーバＢはそのサーバに宛てられた要求のみを受け取ることと、サーバＢ上のトンネル・アプリケーションはファイアウォール内部のポートに宛てられていると思われる要求のみを受け取り、前述のトラステッド・ソケット・テーブル内の現在有効な項目に宛てられている場合にのみ、それらの要求を有効なものとして識別することを理解されたい。

要求が無効な場合、その要求は無視され、サーバＢ（にあるアプリケーション）は再び要求を待つ。しかし、要求が有効な場合、サーバＢ（におけるトンネル・アプリケーション）は、要求側オブジェクトに関してデータ伝送の外部要素を処理するプロセスまたはタスク「Ｂ．１」を作成する（第３図の２３）。タスクＢ．１は、タスクＢ．１自体と要求側オブジェクトとの間のデータ接続を確立し（第３図の２３）、要求をタスクＢ．１の識別情報と共に、制御接続を介してサーバＡ（におけるトンネル・アプリケーション）に転送する（第３図の２４）。

サーバＡ（におけるトンネル・アプリケーション）は、有効性が検証された要求を受け取ると、外部の要求側オブジェクトと要求で識別されているホスト・オブジェクトとの間のデータの伝送の内部態様を処理するプロセスまたはタスクＡ１を生成する（第３図の２５．後者のオブジェクトは後述のトラステッド・ソケット指定の構成要素である）。タスクＡ．１は、ホスト・オブジェクトからファイアウォールまでのデータ接続セグメントを作成し、ファイアウォール・コンピュータにＢ．１までの接続を形成するように指示し（第１図の２５）、したがって、内部ホスト・オブジェクトと外部要求側オブジェクトとの間のデータ接続を完成させる。このデータ接続には、サーバＡおよびＢとファイアウォール・コンピュータ内にデータ伝送プロトコル（以下で詳述）によって定められた容量で、

そのプロトコルに必要な（パケット）伝送速度のバッファが必要な場合があることを理解されたい。

トラステッド・ソケット・テーブルの形式を第４図に示す。３０に２つの特定の項目の例が示されており、３１に２番目の項目から下に延びる点線で追加の項目が暗黙に示されている。各項目は、ポート番号と、伝送プロトコル（通常はバースト・パケット伝送プロトコル）を定義する情報と、ホスト・オブジェクトを識別する情報とから成る。ポート番号は、ホスト・オブジェクトに割り当てられたファイアウォール内部のアドレスである。プロトコルの例として、テーブル内の最初の２項目はＮＮＴＰ（ネットワーク・ニューズ転送プロトコル）とＨＴＴＰ（ハイパーテキスト転送プロトコル）がリストされている。

第５図に、インタフェース・サーバＡおよびＢにあるトンネル・アプリケーションによって実行される詳細な操作を示

す。第２図および第３図に示す操作と同じ操作は同じ番号で識別されている。第２図および第３図に示す操作の一部である操作または何らかの点で異なる操作は、同じ番号の後に英字（ａ、ｂなど）が付いている。その他の操作は前に使用した番号とは異なる番号で識別されている。

サーバＡにおける操作１０ａは、第２図の操作１０と１２の組合せであり、トラステッド・ソケット・テーブルの作成および更新（拡張、修正など）とサーバＢへのトラステッド・ソケット・テーブルのコピーである。サーバＡにおける操作１１ａは、サーバＡとサーバＢ（におけるトンネル・アプリケーション）の間の制御接続の確立または（後述の）再確立である。制御接続の再確立の必要が生じるのは、接続が意図せずに切断された場合であり、そのような事象の検出とそれに対する応用に必要な操作は第５図の４６～４８（これらについては後で詳述する）に示されている。

トラステッド・ソケット・テーブルのコピーを受け取った後、サーバＢ（におけるトンネル・アプリケーション）は外部要求が着信しないか待機する（第５図の２０）。有効な外部トンネル要求を受け取り、そのために付随するデータ処理タスク（たとえば第３図のＢ．１）が作成されると、サーバＢはその要求を、行

われる処置を示す制御信号およびその要求を処理するためにＢで作成されたタスク（たとえばＢ．１）を識別する情報と共に、サーバＡに提示する（第５図の２３ａ）。次に、サーバＢは、サーバＡからの要求受信の肯定応

答を待ち（第５図の２３ｃ）、それを受信すると、サーバＢは、新たに作成されたタスクから要求側オブジェクトまでのデータ接続セグメントを確立する（第５図の２４ｂ。たとえば第３図のＢ．１からＣまで）。次に、サーバＢはファイアウォールからＢで作成されたばかりのタスクまでのデータ接続セグメントが確立するのを待つ（第５図の２４ｃ）。この事象は、ホスト・オブジェクト（要求で識別されているオブジェクト）とサーバＢとの間の関連づけられたデータ接続セグメントの確立を意味する。次に、サーバＢにおけるトンネル・プロセスは、ファイアウォールとタスクＢとの間のデータ接続セグメントが終了するまで完了し（第５図の４０）、この接続およびそれに付随する要求へのサーバＢの関与が終了する（第５図の４１）。

サーバＡでのトンネル処理の考察に戻ると、制御接続の確立または再確立後、サーバＡはＢからの（要求転送）信号が着信しないか待機する（第５図の４６）。まだ信号を受け取っていないが（第５図の４７）、待機が開始されてから所定のタイムアウト間隔がまだ経過していない場合（第５図の４８）、サーバＡはただそのような信号を待ち続けるだけである。しかし、タイムアウトが経過した場合（第５図の４８における肯定の決定）、制御接続が（意図せずに）切断されたものと見なされ、接続が再確立される（１１ａが繰り返される）。

サーバＢから要求を受け取った場合、サーバＡは任意選択

によりそれ独自の妥当性検査操作（第５図の４９）を行って要求が現在有効なトラステッド・ソケットに宛てられたものであることを検証することができる。このオプションを使用し、要求が無効であると判明した場合、サーバＢには２３ｂで待たれていた肯定応答の代わりにエラー信号が返される。このオプションを使用しない場合、またはこのオプションを使用して要求が有効であると判明した場合、サーバＡはＡ．１などの内部タスクの確立に進み、前述のようにこの内部タ

スクがホスト・オブジェクトからファイアウォールまでのデータ接続セグメントを形成し、ファイアウォール・コンピュータに対してデータ接続をＢ．１まで拡張するように指示する（第５図の５０）。これによって、現行要求へのサーバＡの関与が終わり、他の要求に移れるように解放される（第５図の５１）。

プログラム製品

上述のトンネル・アプリケーションは、たとえば記憶媒体または通信ネットワークで、「コンピュータ可読」プログラム製品として配布することができる。このような製品は単一の統合実体（たとえばサーバＡ内部にインストールされ、全体または一部が外部サーバＢに転送されるもの）として、または内部サーバと外部サーバに別々にインストール可能な２つの実体（または部分）として提供することができるものと理解されたい。また、ファイアウォール・コンピュータはファイアウォールを通るデータ接続の形成における必要な関与物であることも理解されたい。

【図１】

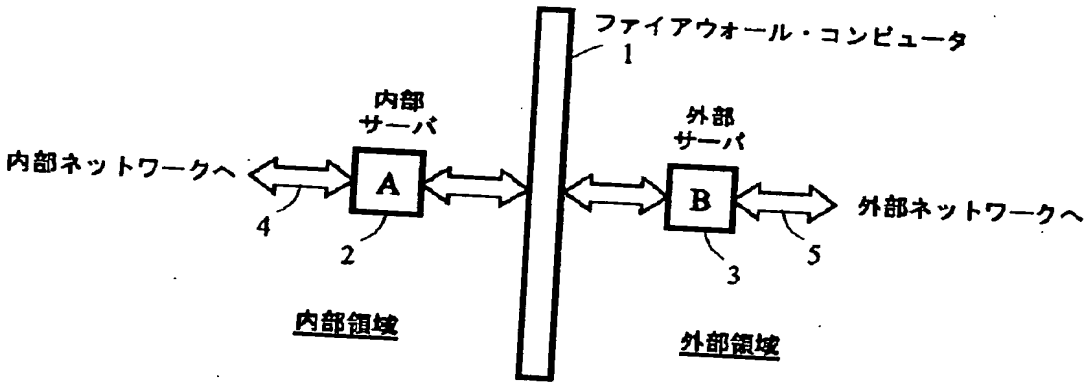



FIG. 1

【図２】

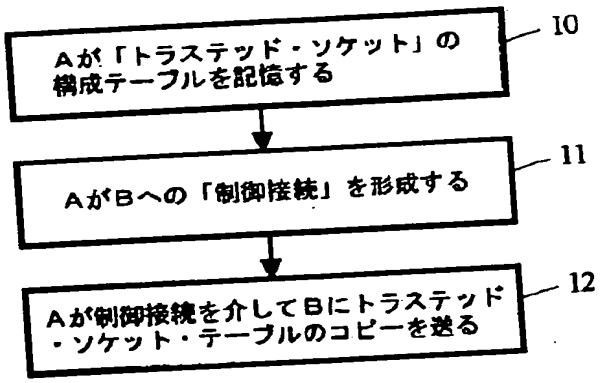



FIG. 2

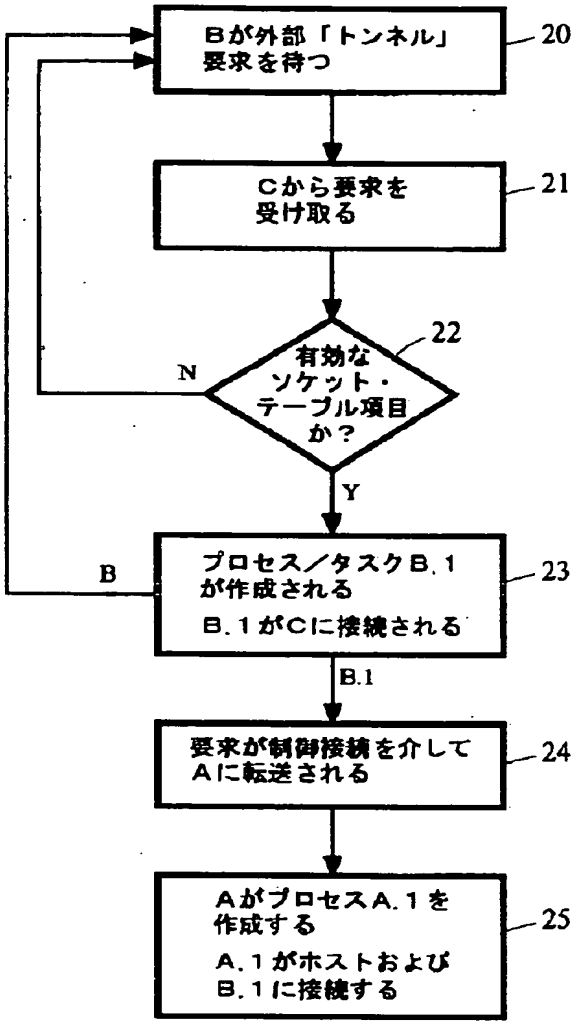
【図４】

| 「トラステッド・ソケット・ポート」 | プロトコル | ホスト ＩＤ |
|---|---|---|
| １１８ | ＮＮＴＰ | ＶＶＵ |
| １１９ | ＨＴＴＰ | ＸＹＺ |
| ・ | ・ | ・ |
| ・ | ・ | ・ |
| ・ | ・ | ・ |

30
31

FIG. 4

【図３】




「結果：ホストとCが接続される（双方向）」

FIG. 3

【図５】

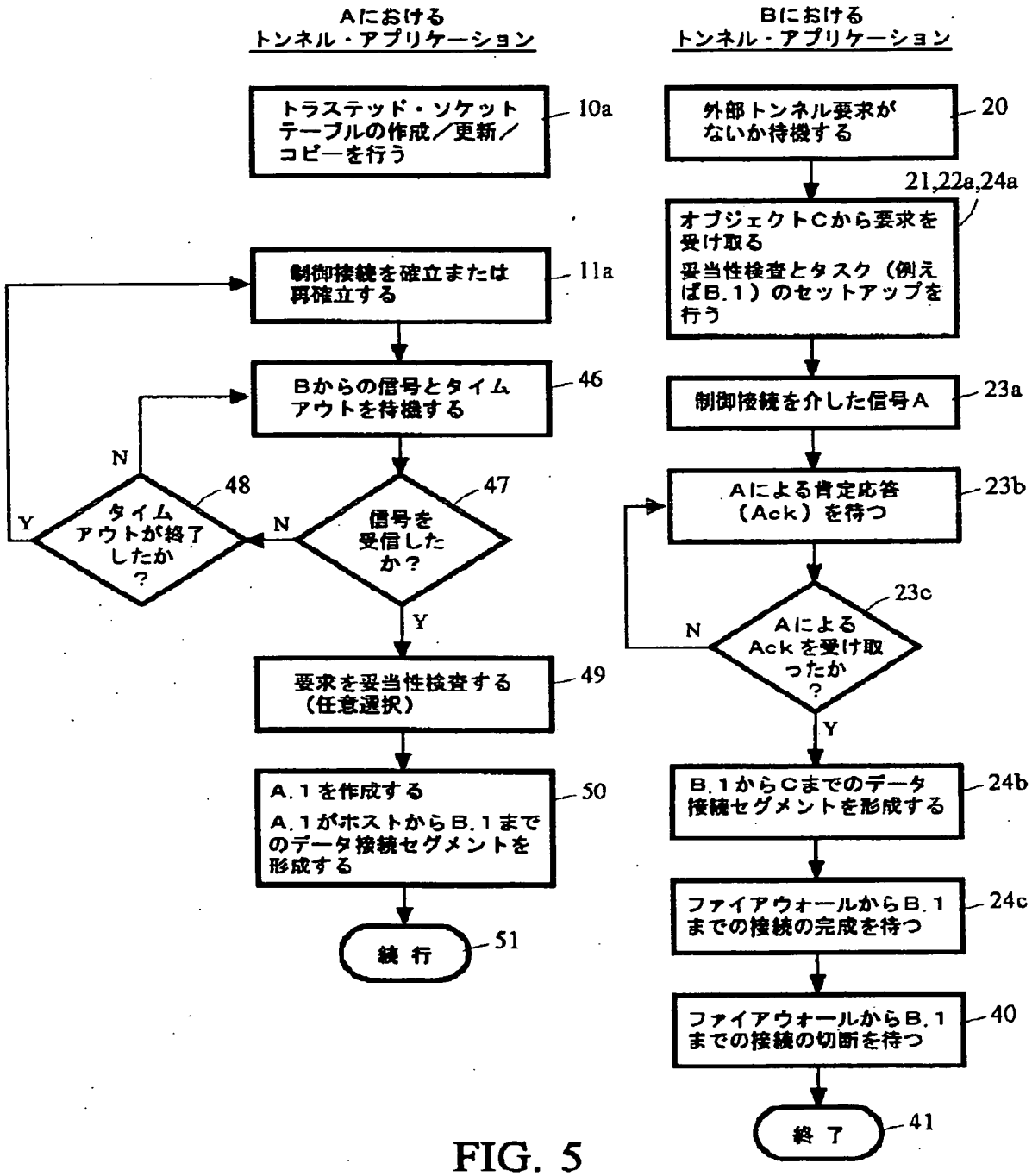

Aにおける
トンネル・アプリケーション
トラステッド・ソケット
テーブルの作成／更新／
コピーを行う
10a
制御接続を確立または
再確立する
11a
Bからの信号とタイム
アウトを待機する
46
信号を
受信した
か？
47
タイム
アウトが終了
したか
？
48
N
Y
N
Y
要求を妥当性検査する
（任意選択）
49
A.１を作成する
A.１がホストからB.１まで
のデータ接続セグメントを
形成する
50
続 行
51
Bにおける
トンネル・アプリケーション
外部トンネル要求が
ないか待機する
20
21,22a,24a
オブジェクトCから要求を
受け取る
妥当性検査とタスク（例え
ばB.１）のセットアップを
行う
制御接続を介した信号A
23a
Aによる肯定応答
（Ack）を待つ
23b
Aによる
Ackを受け取
ったか
？
23c
N
Y
B.１からCまでのデータ
接続セグメントを形成する
24b
ファイアウォールからB.１
までの接続の完成を待つ
24c
ファイアウォールからB.１
までの接続の切断を待つ
40
終 了
41

FIG. 5

【手続補正書】

【提出日】１９９９年４月１４日（１９９９．４．１４）

【補正内容】

請求の範囲

１．ファイアウォールが内部領域と外部領域を規定し、前記外部領域内のオブジェクトが前記内部領域内のオブジェクトへのアクセスを直接開始するのを防止するセキュリティ障壁を形成すると同時に、前記内部領域内のオブジェクトが前記外部領域内のオブジェクトへのアクセスを直接開始し、アクセスを獲得することを許すファイアウォール（１）を含むデータ通信ネットワークのためのトンネル装置であって、

前記ファイアウォール（１）と前記外部領域内のオブジェクトとの間のインタフェースをとる、前記外部領域内の外部インタフェース・コンピュータ（３）と、

前記ファイアウォール（１）と前記内部領域内のオブジェクトとの間のインタフェースをとる、前記内部領域内の内部インタフェース・コンピュータ（２）と、

前記内部と外部の両方のインタフェース・コンピュータにおいて、前記外部領域からのアクセスが許可されている前記内部領域内の所定のトラステッド・オブジェクトの識別情報を確認する手段と、

前記外部インタフェース・コンピュータにおいて、前記外部領域内のオブジェクトから送られた要求に応答して、前記確認手段と協調して、前記要求が前記トラステッド・オブジェクトのうちの１つのオブジェクトに宛てられたものであるか否かを判断し、前記要求がそのように宛てられたものである場合、前記要求を前記内部インタフェース・コンピュータにルーティングする手段と、

前記内部と外部の両方のインタフェース・コンピュータにおいて、前記トラステッド・オブジェクトのうちの前記１つのオブジェクトに宛てられた前記要求に応答して、前記トラステッド・オブジェクトのうちの前記１つのオブジェクトとそれぞれの前記要求を送った外部オブジェクトとの間のデータ通信接続を形成す

る手段とを含み、前記データ通信接続のうちの前記内部領域にあるセグメントと前記ファイアウォールを通って延びるセグメントが前記内部インタフェース・コンピュータの排他的制御下で形成され、前記データ通信接続のうちの前記外部インタフェース・コンピュータから前記要求を送った前記オブジェクトまでのセグメントが前記外部インタフェース・コンピュータの制御下で形成され、

前記内部インタフェース・コンピュータが、前記外部インタフェース・コンピュータへの専用制御接続の確立と維持を行う手段を含み、前記専用制御接続が前記要求を前記外部インタフェース・コンピュータから前記内部インタフェース・コンピュータに伝送するために使用されるトンネル装置。

２．前記トラステッド・オブジェクトの識別情報を確認する前記手段が、前記内部インタフェース・コンピュータにおいて、前記トラステッド・オブジェクトをリストするテーブル（第４図）の作成と維持を行う手段と、前記テーブル・リストのコピーを前記ファイアウォール（１）を介して前記外部インタフェース・コンピュータ（３）に転送する手段と、前記外部インタフェース・コンピュータにおいて、前記コピーされたテーブル・リストの記憶と参照を行う手段とを含む、請求項１に記載のトンネル装置。

３．トラステッド・オブジェクトの前記テーブル内の各項目（３０）が、前記内部領域内のオブジェクトを識別する第１の情報と、それぞれの前記オブジェクトに割り当てられたデータ通信ポートを識別する第２の情報と、前記ポートを介してデータを伝送するために使用されるデータ通信プロトコルを識別する第３の情報とから成る、請求項２に記載のトンネル装置。

４．前記トラステッド・オブジェクトの識別情報を確認する前記手段と、データ通信接続を形成する前記手段とが、

前記内部と外部の両方のインタフェース・コンピュータ内で実行され、前記確認手段と前記形成手段を構成要素として含む、トンネル・アプリケーション・プログラムと、

前記要求を前記内部インタフェース・コンピュータにルーティングする前記手段が、前記トンネル・アプリケーション・プログラムの第３の構成要素を含む、

請求項１に記載のトンネル装置。

５．前記内部領域と外部領域がそれぞれ内部および外部のデータ通信ネットワークを含み、前記内部および外部のインタフェース・コンピュータが前記ファイアウォールと前記内部

ネットワークおよび外部ネットワークのノードとの間にそれぞれ接続された、請求項１に記載のトンネル装置。

６．ファイアウォール外部のデータ処理オブジェクトが前記ファイアウォール内部のデータ処理オブジェクトとのデータ通信接続を確立することができるようにする、コンピュータ可読記憶媒体上に記憶されたトンネル・ソフトウェアであって、

それぞれ前記ファイアウォールの内部と外部に配置され、前記ファイアウォールとそれぞれ前記ファイウォールの内部と外部にある前記オブジェクトとの間のインタフェースをとるコンピュータ上で実行されるように意図された内部および外部のプログラム・セグメントを含み、

前記内部セグメントが、前記内部コンピュータを操作してトラステッド内部オブジェクトのテーブルの作成と維持を行う手段と、前記ファイアウォールと共に前記内部コンピュータを操作して前記外部セグメントに前記テーブルのコピーを供給する手段とを含み、

前記内部セグメントが、前記外部セグメントへの専用制御接続の確立と維持を行う手段を含み、前記専用制御接続が前記外部セグメント内のオブジェクトから送られた要求を前記外部セグメントから前記内部セグメントに伝送するために使用されるトンネル・ソフトウェア。

７．コンピュータ・システム・セキュリティ・ファイアウォール（１）外部のオブジェクトが前記ファイアウォール内部

の選択されたオブジェクトへのデータ接続を獲得することができるようにする方法であって、

テーブル内の各項目（３０）が選択されたオブジェクトと前記オブジェクトに

割り当てられたデータ通信ポートとそれぞれの前記ポートに割り当てられたデータ通信プロトコルとを識別する情報を含む、前記ファイアウォール（１）内部の選択されたオブジェクトのテーブルの作成と維持を行うステップと、

前記ファイアウォール外部に前記テーブルのコピーを設けるステップと、

外部オブジェクトに前記テーブル内の項目を構成する情報への特定のセキュリティ・クリアランス・アクセスを与えるステップと、

それぞれの前記外部オブジェクトに、前記外部オブジェクトに提供された情報によって規定された前記オブジェクト、ポート、およびプロトコル・エンティティへのアクセスを求める要求を発行させるステップと、

前記ファイアウォールの外部と内部のコンピュータ・システムに、各要求で識別された特定の内部オブジェクトと前記要求を発行した外部オブジェクトとの間にデータ伝送接続を確立させるステップとを含み、前記データ伝送接続のうちの前記ファイアウォールの内部にあるセグメントと前記ファイアウォールを通って延びるセグメントが前記ファイアウォールの内部の前記コンピュータ・システムの排他的制御下で形

成され、

前記ファイアウォール内部の前記コンピュータ・システムが前記ファイアウォール外部のコンピュータ・システムへの専用制御接続の確立と維持を行い、前記専用制御接続が前記ファイアウォール外部の前記コンピュータ・システムから前記ファイアウォール内部の前記コンピュータ・システムに前記要求を伝送するために使用される方法。

【国際調査報告】

# INTERNATIONAL SEARCH REPORT

Intr ‘tional Application No
PCT/GB 97/02712

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| P,X | WO 97 16911 A (IBM ;IBM UK (GB)) 9 May 1997<br>see page 1, line 36 - page 2, line 40<br>see page 4, line 9 - page 5, line 38 | 1,3,5,6 |
| P,A | see page 7, line 6 - page 8, line 37<br>see page 12, line 4 - line 37<br>see claims 1,2,6,7,9-12; figures 1,3<br>---<br>-/— | 2,4,7-9 |

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 4 December 1997 | 23/12/1997 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Karavassilis, N |

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Inte tional Application No
PCI/GB 97/02712

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CHESWICK AND BELLOVIN: "Firewalls and Internet Securuty, repelling the Willy Hacker" April 1994 , ADDISON-WESLEY PUBLISHING COMPANY XP002049117 | 1,2,4-9 |
| A | Pages 86 to 106 see page 87 - page 89, line 2; figure 4.1 see page 93, paragraph 4.4.2 - page 94, line 9 see page 94, paragraph 4.5.1 - page 98; figure 4.2 | 3 |
| X | BRYAN J: "FIREWALLS FOR SALE" BYTE, vol. 20, no. 4, 1 April 1995, page 99/100, 102, 104 XP000501822 | 1,5,6 |
| A | see page 100, column 3, line 35 - page 102, column 2, line 3; figure 3 (Figure titled Digital's Three-Way Isolation) | 2-4,7-9 |
| X | TED DOTY: "A FIREWALL OVERVIEW" CONNEXIONS, vol. 9, no. 7, 1 July 1995, pages 20-23, XP000564023 | 1,5 |
| A | (especially Paragraphs "Circuit Relay Firewalls", "Which Firewalls are best" and figure 1) see the whole document | 2-4,6-9 |
| A | BELLOVIN S M ET AL: "NETWORK FIREWALLS" IEEE COMMUNICATIONS MAGAZINE, vol. 32, no. 9, 1 September 1994, pages 50-57, XP000476555 (especially paragraphs "Circuit level gateways", "Supporting Inbound Services" and "Tunnels Good and Bad") see page 6, column 1, line 56 - page 7, column 2, line 69 | 1-9 |
| A | NEWMAN D ET AL: "CAN FIREWALLS TAKE THE HEAT?" DATA COMMUNICATIONS, vol. 24, no. 16, 21 November 1995, pages 71-78, 80, XP000576579 | |
| A | NORITOSHI DEMIZU ET AL: "DDT - A VERSATILE TUNNELING TECHNOLOGY" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 27, no. 3, 1 December 1994, pages 493-502, XP000483281 | |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 97/02712

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| WO 9716911 A | 09-05-97 | NONE | |

フロントページの続き

(72)発明者 ラオ、アルン、モハン
アメリカ合衆国テキサス州ダラス、シェイディブルック・レーン 6301
(72)発明者 ウォルターズ、グレン、ロバート
アメリカ合衆国フロリダ州セブリング、アストリア・アベニュー 3208

【要約の続き】
すると同時に、そのような接続を行う許可に伴うセキュリティ上のリスクを最小限にする。この機構は、ファイアウォールの内部と外部のインターフェイス・サーバ上で実行される特別なトンネル・アプリケーションと、内部トンネルアプリケーションによって作成され、維持される「トラステッド・ソケット」の特別なテーブルとを含む。トラステッド・ソケット・テーブル内の項目は、ファイアウォール内部のオブジェクトを規定し、特別な内部ポートと、各ポートで使用される通信プロトコルと、各ポートに関連づけられたホスト・オブジェクトとから成る。各項目は、外部からファイアウォールを通過する「トンネル」アクセス権を持つことを許可された個人にしかわからないと考えられるという意味で「トラステッド」である。これらのアプリケーションは、有効なテーブル項目を識別した外部要求に応答して、テーブルを使用してファイアウォールを介した接続を行う。

閉じる

集合：7　　件数：74　　しおり選択分：2件　　1件目～1件目

*00001*

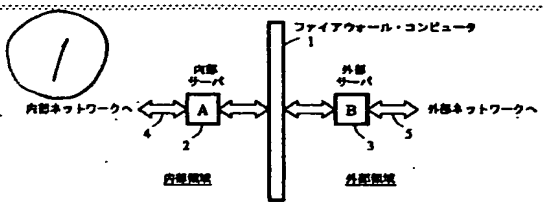



FIG. 1

【公報種別】公表特許公報
【公表番号】特表2000-505270　平成12年(2000)4月25日
【発明の名称】ファイアウォールを《通過》するコンピュータ資源への外部アクセス
【ＩＰＣ】H04L 12/66, G06F 13/00-351, H04L 12/28, H04L 12/46, H04L 12/56
【ＦＩ】H04L 11/20-B, G06F 13/00-351-Z, H04L 11/20-102-Z, H04L 11/00-310-C
【出願番号】特願平10-519056　平成9年(1997)10月2日
【国際出願番号】PCT/GB97/02712
【国際公開番号】WO98/18248　平成10年(1998)4月30日
【優先権】08/731,800　平成8年(1996)10月21日　米国(US)
【指定国】EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), BR, CA, CN, CZ, HU, JP, KR, PL, RU
【出願人】インターナショナル・ビジネス・マシーンズ・コーポレーション；
【発明者】ジェイド、プラシャント；　ムーア、ビクター、スチュアート；　ラオ、アルン、モハン；　ウォルターズ、グレン、ロバート；
【要約】　ファイアウォールが、ファイアウォール内部のコンピュータ資源およびネットワーク資源を、ファイアウォール外部のコンピュータおよびコンピュータ・アプリケーションから分離する。典型的には、内部資源は私有データベースおよびローカル・エリア・ネットワーク（ＬＡＮ）が考えられ、外部オブジェクトは《インターネット》などの公衆通信ネットワークを介して操作する個人およびコンピュータ・アプリケーションを含む。
通例、ファイアウォールは内部のユーザまたはオブジェクトが外部のオブジェクトまたはネットワークへの接続を開始することはできるようにするが、その逆方向、すなわち外部から内部への接続は行われないようにする。
開示の本発明は、ファイアウォールの両側で動作し、ファイアウォール外部の特定の「トラステッド」個人、オブジェクト、またはアプリケーションによって要求された場合に、そのような「外部から内部への」接続を確立する特別な「トンネル」機構を提供する。
本発明の意図は、「トンネル」接続（外部から有効に要求されたファイアウォールを介した接続）を確立するのに必要な資源を最小限にすると同時に、そのような接続を行う許可に伴うセキュリティ上のリスクを最小限にする。
この機構は、ファイアウォールの内部と外部のインターフェイス・サーバ上で実行される特別なトンネル・アプリケーションと、内部トンネルアプリケーションによって作成され、維持される「トラステッド・ソケット」の特別なテーブルとを含む。
トラステッド・ソケット・テーブル内の項目は、ファイアウォール内部のオブジェクトを規定し、特別な内部ポートと、各ポートで使用される通信プロトコルと、各ポートに関連づけられたホスト・オブジェクトとから成る。
各項目は、外部からファイアウォールを《通過》する「トンネル」アクセス権を持つことを許可された個人にしかわからないと考えられるという意味で「トラステッド」である。
これらのアプリケーションは、有効なテーブル項目を《識別》した外部要求に応答して、テーブルを使用してファイアウォールを介した接続を行う。